34. Class Number One Criteria For Real Quadratic Fields. I

By R. A. MOLLIN
Mathematics Department, University of Calgary,
Calgary, Alberta, Canada, T2N 1N4

(Communicated by Shokichi IYANAGA, M. J. A., April 13, 1987)

In [5] we established criteria for $Q(\sqrt{n})$ to have class number, $h(n)$, equal to one when $n=m^2+1$ is square-free. Portions of this result were rediscovered by Yokoi [15] and Louboutin [4], both of whom also found similar criteria for square-free integers of the form $n=m^2+4$. It is the purpose of this paper to generalize all of the above by providing criteria for $h(n)=1$ for a positive square-free integer $n\equiv 1 \pmod 4$, under a certain assumption, which is satisfied (among others) by Richaud-Degert (R-D) types described below. One of these criteria is that $-x^2+x+(n-1)/4$ is equal to a prime for all integers $x\in(1, (\sqrt{n}-1)/2)$. This is the exact real quadratic field analogue of: $h(-p)=1$ if and only if $x^2-x+(p+1)/4$ is prime for all integers $x\in[1, (p-7)/4]$ where $p\equiv 3 \pmod 4$ is prime and $p>7$. This was proved by Rabinowitsch [10] (see also [1], [12], and [13]).

We apply the criteria to real quadratic fields of narrow R-D type; i.e., those $n=m^2+r$ where $|r|\in\{1,4\}$, $n\neq 5$. We also observe that when $n=m^2+4$ the existence of exactly six quadratic fields with $h(n)=1$ can be established by the same method used by Mollin and Williams in [9] to verify a similar fact for the case $n=m^2+1$.

The following notation is in force throughout the paper. For the field $Q(\sqrt{n})$ we denote the fundamental unit by $(T+U\sqrt{n})/\sigma$, $\sigma=2$ if $n\equiv 1$ (mod 4), and $\sigma=1$ otherwise. Moreover $N((T+U\sqrt{n})/\sigma)=\delta$ where N denotes the norm from $Q(\sqrt{n})$ to Q. For convenience' sake we let $A=((2T/\sigma)-\sigma-1)/U^2$.

First we state the following result which we will need for the first main theorem. The proof of the following can be found in [5] (see also [8]).

Lemma. *Let n be a square-free positive integer. If $h(n)=1$ then p is inert in $Q(\sqrt{n})$ for all primes $p<A$.*

The converse of this Lemma is clearly false. For example, if $n=34$ then $\sigma=1$, $T=35$, $U=6$, and $\delta=1$ so $A=68/36<2$. However, $h(34)=2$. However, the converse does hold under certain circumstances, as the following main result illustrates.

Theorem. *Let $n\equiv 1$ (mod 4) be a positive square-free integer, such that $(\sqrt{n}-1)/2\leq A$. Then the following are equivalent.*

(1) $h(n)=1$;

(2) *p is inert in $Q(\sqrt{n})$ for all primes $p<A$;*

(3) *$f(x)=-x^2+x+(n-1)/4\not\equiv 0 \pmod p$ for all integers x and primes p satisfying $0<x<p<(\sqrt{n}-1)/2$;*

(4) *$f(x)$ is equal to a prime for all integers x such that $1<x<(\sqrt{n}-1)/2$.*

Proof. (2) follows from (1) by the Lemma; (note that in this case $(\sqrt{n}-1)/2\le A$ is not required). Assume now that (2) holds. If $f(x)\equiv 0 \pmod p$ for some $0<x<p<(\sqrt{n}-1)/2$ then $n\equiv(2x-1)^2 \pmod p$; whence p is not inert in $Q(\sqrt{n})$. By (2) this forces $(\sqrt{n}-1)/2>A$, contradicting the hypothesis. Thus (2) implies (3).

Assume (3) holds. If $(n-1)/4$ is composite, but not the square of a prime, then there exists a prime p dividing $(n-1)/4$ such that $f(1)\equiv 0 \pmod p$ with $0<1<p<(\sqrt{n}-1)/2$. This contradicts (3). Hence for some prime p we must have that $(n-1)/4=p$ or p^2.

Suppose that there are primes p_1 and p_2 (not necessarily distinct) such that $f(x)\equiv 0 \pmod{p_1p_2}$ for some integer x with $1<x<(\sqrt{n}-1)/2$. If $p_1p_2\ge(n-1)/4$ then $-x^2+x+(n-1)/4\ge(n-1)/4$; whence $x\le 1$, a contradiction. Therefore, without loss of generality we may assume that $p_1<(\sqrt{n}-1)/2$. If p_1 divides x then p_1 divides $(n-1)/4$; whence $p_1=p$. However we have that $p=p_1\le x<(\sqrt{n}-1)/2\le p$, a contradiction. Hence, in consideration of the congruence $f(x)\equiv 0 \pmod{p_1}$ we may assume without loss of generality that $0<x<p_1$. Hence, we have $f(x)\equiv 0 \pmod{p_1}$ with $0<x<p_1<(\sqrt{n}-1)/2$ which contradicts (3). Thus (3) implies (4).

Finally assume that (4) holds. If $h(n)>1$ then by [3, Propositions 3 and 4, p. 126] there exist an integer x and a prime p such that $0\le x<p\le(\sqrt{n}-1)/2$ and both:

(a) $N((2x-1-\sqrt{n})/2)\equiv 0 \pmod p$ and

(b) there does not exist an integer k such that $|N(2x+2kp-1-\sqrt{n})/2|<p^2$.

From (a) it follows that $-x^2+x+(n-1)/4\equiv 0 \pmod p$. Therefore, if $1<x<(\sqrt{n}-1)/2$ then, by (4), $-x^2+x+(n-1)/4=p$. However $x<p\le(\sqrt{n}-1)/2$; whence $p=x(1-x)+(n-1)/4>p(1-p)+p^2=p$, a contradiction. Hence $x=0$ or 1. Therefore p divides $(n-1)/4$; whence $f(p)=p(-p+1+(n-1)/4p)$. If $p<(\sqrt{n}-1)/2$ then (4) implies that $f(p)=p$. Thus $p=(\sqrt{n}-1)/2$, a contradiction. Hence $p=(\sqrt{n}-1)/2$. Setting $k=1$ in (b) yields that: $p^2\le|N(2p\pm 1-\sqrt{n})/2|=|(4p^2\pm 4p+1-n)/4|=p$, a contradiction. This secures the result. Q.E.D.

The following special case of the Theorem for certain R-D type was proved in [5]. It was also rediscovered by Yokoi [15] and Louboutin [4]. See also [7].

Corollary 1. *If $n=4l^2+1$ is square-free where either n is composite or l is composite then $h(n)>1$. If $n=4q^2+1$ where n and q are primes then the following are equivalent:*

(1) *$h(n)=1$;*

(2) *p is inert in $Q(\sqrt{n})$ for all primes $p<q$;*

(3) $f(x)=-x^2+x+q^2\not\equiv 0 \pmod p$ *for all integers* x *and primes* p *such that* $0<x<p<q$;

(4) $f(x)$ *equals a prime for all* x *with* $1<x<q$.

Proof. By [2] and [11] $T=4l$ and $U=2$. Moreover, $\delta=-1$, $(\sqrt{n-1})/2=l$ and $A=l$. Thus the hypothesis of the theorem is satisfied. Q.E.D.

S. Chowla conjectured that if $p=m^2+1$ is prime with $m>26$ then $h(p)>1$. Thus Corollary 1 reduces the conjecture to the case where $m=2q$, $q>13$ prime. This exhausts the algebraic techniques (see [5]). Using analytic techniques and the generalized Riemann hypothesis, Mollin and Williams proved the Chowla conjecture in [9].

We now turn to another interesting consequence of the Theorem. The following R-D types were also considered by Yokoi [15] and Louboutin [4]. Both of these authors' results follow as a special case of the following.

Corollary 2. *Let* $n=m^2\pm 4>5$ *be square-free. Then* $h(n)>1$ *unless* $n=4p+1$ *where* p *is prime. In this case the following are equivalent*:

(1) $h(n)=1$;

(2) q *is inert in* $Q(\sqrt{n})$ *for all primes* $q<\begin{cases} m & \text{if } n=m^2+4 \\ m-2 & \text{if } n=m^2-4 \end{cases}$;

(3) $f(x)=-x^2+x+p\not\equiv 0 \pmod q$ *for all integers* x *and primes* q *satisfying* $0<x<q<\sqrt{p}$;

(4) $f(x)$ *is equal to a prime for all integers* x *satisfying* $1<x<\sqrt{p}$.

Proof. By [2] and [11] $T=m$ and $U=1$. An easy check shows that $(\sqrt{n-1})/2\le A$. Thus the hypothesis of the Theorem is satisfied, and the equivalence (1)–(4) is secured. It remains to show that $h(n)>1$ unless $n=m^2\pm 4=4p+1$ where p is prime.

Suppose that $(n-1)/4$ is not prime and $h(n)=1$. Then (3) of the Theorem implies, by the same reasoning as in the proof of the Theorem, that $(n-1)/4=p^2$ for some prime p. Therefore $m^2-4p^2=5$ (respectively $m^2-4p^2=-3$) when $n=m^2-4$ (respectively $n=m^2+4$). In the former case $m+2p=5$ is forced, contradicting $m>3$; and in the latter case $m-2p=-3$ is forced, contradicting $m>1$. This shows that $n=4p+1$ for some prime p when $h(n)=1$. Q.E.D.

Remark 1. In [15] Yokoi conjectured that $h(n)>1$ when $n=q^2+4$ is square-free with $q>17$ prime. Under the assumption of the generalized Riemann hypothesis this conjecture follows in the same fashion as did the analogous Chowla conjecture proved by Mollin and Williams in [9].

Remark 2. Suppose that $n=4p+1=m^2+4$ where p is a prime and m is a positive integer. If $s<\sqrt{p}$ is an odd prime then $p\equiv t \pmod s$ for $0\le t<s$. If there exists an integer $u>0$ such that $1+4t\equiv(2u-1)^2 \pmod s$ then $f(u)=-u^2+u+p\equiv 0 \pmod s$ where $0<u<s<\sqrt{p}$. This violates condition (3) of Corollary 2. Hence $h(n)>1$. (See [6] for connections with generalized Fibonacci primitive roots.)

The following Table illustrates Corollaries 1–2. We list the $r=1$ case only up to $m=26$ since we know by Remark 1 that $h(n)>1$ for $m>26$. Similarly we list the $r=4$ only up to $m=17$. For $r=-4$ with $h(n)=1$ it is unlikely that any other such n exist than those listed in the Table.

Table. $n=m^2+r$

m	r	n	$h(n)$
6	1	37	1
8	1	65	2
10	1	101	1
12	1	145	4
14	1	197	1
16	1	257	3
20	1	401	5
22	1	485	2
26	1	677	1
5	4	29	1
7	4	53	1
9	4	85	2
13	4	173	1
15	4	229	3
17	4	293	1
5	−4	21	1
9	−4	77	1
21	−4	437	1
309	−4	95477	11

All class numbers are taken from [14].

In a subsequent work we will look at *wide* R-D types in detail.

Acknowledgement. This research was supported by both N.S.E.R.C. Canada Grant ♯A8484 and an I. W. Killam Award held at the University of Calgary in 1986.

References

[1] R. G. Ayoub and S. Chowla: On Euler's Polynomial. J. Number Theory, **13**, 443–445 (1981).

[2] G. Degert: Über die Bestimmung der Grudeinheit gewisser reell-quadratischer Zahlkörper. Abh. Math. Sem. Univ. Hamburg, **22**, 92–97 (1958).

[3] M. Kutsuna: On a criterion for the class number of a quadratic number field to be one. Nagoya Math. J., **79**, 123–129 (1980).

[4] S. Louboutin: Critères des principalité et minoration des nombres de classes l'idéaux des corps quadratiques réels à l'aide de la théorie des fractions continues (preprint).

[5] R. A. Mollin: Necessary and sufficient conditions for the class number of a real quadratic field to be one, and a conjecture of S. Chowla (to appear in Proc. Amer. Math. Soc.).

[6] ——: Generalized Fibonacci primitive roots, and class numbers of real quadratic fields (to appear in The Fibonacci Quarterly).

[7] ——: Diophantine equations and class numbers. J. Number Theory, **24**, 7–19 (1986).

[8] R. A. Mollin: On the insolubility of a class of diophantine equations and the non-triviality of the class numbers of related real quadratic fields of Richaud-Degert type (to appear in Nagoya Math. J.).

[9] R. A. Mollin and H. C. Williams: A conjecture of S. Chowla via the generalized Riemann hypothesis (to appear in Proc. Amer. Math. Soc.).

[10] G. Rabinowitsch: Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern. J. Rein Angew Math., **142**, 153–164 (1913).

[11] C. Richaud: Sur la résolution des équations $x^2-Ay^2=\pm 1$. Atti. Accad. Pontif. Nuovi Lincei, 177–182 (1866).

[12] R. Sasaki: On a lower bound for the class number of an imaginary quadratic field. Proc. Japan Acad., **62A**, 37–39 (1986).

[13] H. M. Stark: A complete determination of the complex quadratic fields of class-number one. Michigan Math. J., **14**, 1–27 (1967).

[14] H. Wada: A table of ideal class numbers of real quadratic fields. Kokyuroku in Math., **10**, Sophia University, Tokyo (1981).

[15] H. Yokoi: Class-number one problem for certain kinds of real quadratic fields (preprint series #7, Nagoya University (1986)).